CI1007 - Cronograma 2026/2

- As atividades indicadas com ! serão avaliadas;
- Os projetos devem ser entregues usando o Moodle.
- Leia com atenção as Regras das Atividades de Laboratório.
- Os trabalhos podem ser feitos em grupos com até **3 pessoas**.

Regras de avaliação

A média final da disciplina é calculada com as notas das provas e dos trabalhos solicitados (entre 0 e 100), da seguinte forma:

```
Média = (P1 + P2 + MT) / 3
P1: prova do 1º bimestre
P2: prova do 2º bimestre
MT: média dos trabalhos (o trabalho sobre ataques tem peso 3, os demais têm peso 1)
```

05/8: Aula 1

- Apresentação da disciplina
- Conceitos básicos
- Conteúdo complementar:
  - Computer security, C. Landwehr, 2001
  - Basic Concepts and Taxonomy of Dependable and Secure Computing. A. Avizienis et al, 2004
  - A Review of Information Security Principles, 1997

07/8: Aula 2

- Conceitos básicos (cont.)
- ! Atividade: Base de Vulnerabilidades (prazo: aula 5)

12/8: Aula 3

- Criptografia: conceitos básicos; algoritmos simétricos
- Atividade em sala sobre cifradores simétricos

14/8: Aula 4

- Criptografia: algoritmos assimétricos
- ! Atividade: O algoritmo RSA (não precisa fazer o 3.6) (prazo: aula 7)
- Conteúdo complementar:
  - Video: Acordo de chaves de Diffie-Hellman (video 1, video 2)

    - Texto: How RSA Works with Examples
    - Vídeo: o algoritmo RSA (video 1, video 2)
    - Vídeo: Elliptic Curves Cryptography

19/8: Aula 5

- Criptografia: resumo criptográfico; assinatura digital; certificado de chave pública; infraestrutura de chaves públicas.
- Exemplos de certificados
- Conteúdo complementar:
    - Certificate MITM attack 1, 2011
    - Certificate MITM attack 2, 2019

21/8: Aula 6

- Atividade: Certificados digitais **Lab 1-2 do DINF**
- Conteúdo complementar: Modelos de criptografia de chave pública alternativos. Goya et al, minicurso do SBSeg 2009.

26/8: Aula 7

- Autenticação: usuários e grupos; técnicas de autenticação; senhas; senhas descartáveis
- Definir Tópicos em autenticação para os seminários
- Leitura complementar:
    - The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes, IEEE Symposium on Security and Privacy, 2012.
    - Designing Password Policies for Strength and Usability, Shay et al, 2016.
    - Método Diceware
    - TOTP

28/8: Aula 8

- Atividade: Quebra de senhas **Lab 1-2 do DINF**
- Leitura complementar: Password cracking

02/9: Aula 9

- Autenticação: desafio/resposta; técnicas biométricas
- Leitura complementar:
    - Introdução à Biometria. Costa et al, SBSeg 2006.

04/9: Aula 10

- Infraestruturas de autenticação; Kerberos
- Leitura complementar:
    - Gerenciamento de Identidades Federadas. Wangham et al, SBSeg 2010.

09/9: Aula 11

- Atividade: seminários sobre Tópicos em autenticação

11/9: Aula 12

- Atividade: seminários (cont.)

23/9: Aula 13

- Atividade: seminários (cont.)

25/9: Aula 14

- Prova 1 (conteúdo: conceitos básicos, criptografia, autenticação)

30/9: Aula 15

- Controle de acesso: políticas, modelos e mecanismos de controle de acesso; políticas discricionárias; políticas obrigatórias
- Definir Tópicos em controle de acesso para os seminários

02/10: Aula 16

- Controle de acesso: políticas baseadas em domínios; políticas baseadas em papéis; políticas baseadas em atributos.
- Controle de acesso: mecanismos de controle de acesso: infraestrutura básica, controle de acesso em UNIX, controle de acesso em Windows
- Leitura complementar:
  - RBAC: Role-Based Access Controls, 1992; Role-Based Access Control Models, 1996.
  - ABAC: Guide to Attribute Based Access Control (ABAC) Definition and Considerations, 2014.
  - UCON: The UCONabc usage control model, 2004.

07/10: Aula 17

- Controle de acesso: mudança de privilégios
- Credenciais de um processo em UNIX: credentials.c

09/10: Aula 18

- Atividade: seminários sobre Tópicos em controle de acesso

14/10: Aula 19

- Atividade: seminários (cont.)

16/10: Aula 20

- Atividade: seminários (cont.)

30/10: Aula 21

- Auditoria: coleta de dados; análise de dados; auditoria preventiva
- Leitura complementar:
  - NIST Guide to Intrusion Detection and Prevention Systems (IDPS), 2007
  - Intrusion Detection Systems: A Survey and Taxonomy, 2000.
- Exemplos de NIDS: Suricata, Snort, Kismet
- Exemplos de HIDS: OSSEC, Samhain, TripWire
- Exemplo de IPS: Fail2ban

04/11: Aula 22

- Segurança baseada em hardware

06/11: Aula 23

- Segurança baseada em hardware (cont.)

11/11: Aula 24

Fix Me! A definir

13/11: Aula 25

Fix Me! A definir

18/11: Aula 26

- ! Atividade: demonstrações de ataques

25/11: Aula 27

- Demonstrações de ataques (cont.)

27/11: Aula 28

- Demonstrações de ataques (cont.)

02/12: Aula 29

- Demonstrações de ataques (cont.)

04/12: Aula 30

- Prova 2 (conteúdo: controle de acesso, auditoria, redes, hardware)

09/12: Exame final
